FORESCOUT

Active Defense for the Enterprise of Things.

Electric Utilities

Optimize risk management and accelerate compliance for Electric Utilities

In the power and utility space, security and operations teams receive thousands of alerts per day across various security tools and dashboards. Among the many cybersecurity challenges associated with protecting the power grid, three of the most difficult are:

- Maintaining an accurate, up-to-date asset inventory
- Analyzing alerts and reducing the mean time to respond (MTTR)
- Complying with regulatory requirements such as the NERC CIP standards in North America and the NIS Directive in Europe

> **In 2019, 56% of utility companies reported that they suffered one or more shutdowns or losses of operational data per year.[1]**

Forescout eyeInspect: The Cyber Resilience Platform for Electric Utilities:

Forescout eyeInspect (formerly SilentDefense™) provides passive and selective active discovery capabilities that create an automatic, real-time asset inventory while also protecting ICS networks from a wide range of threats with patented deep packet inspection (DPI) and anomaly detection technology. eyeInspect helps you streamline threat analysis and incident response with an advanced alert aggregation function that correlates alerts into groups, rapidly reducing the risk of human error and accelerating incident response.

In addition to threat detection and response, eyeInspect helps automate compliance auditing and policy enforcement tasks. Asset owners can easily baseline individual devices and device groups by establishing unique policies to automate deviation detection using the optional eyeInspect active sensor. For example, easily generate admissible proofs/reports of the baseline for NERC CIP audits or NIS Directive requirements.

For customers looking to localize eyeInspect to their analysts' language of choice, eyeInspect allows asset owners to choose from 12 different languages by simply dragging and dropping a file, thus providing the capacity to translate UI messages, date formatting and number formatting to your language of choice.

eyeInspect Use Cases for Utility ICS Networks

Accelerate alert analysis

Create multidimensional alert groups to make it easier to uncover trends in the network. Functioning similar to a pivot table, eyeInspect aggregates alerts by multiple dimensions according to source IP, type of vulnerability, sensor, etc. This provides a powerful, UX-friendly version of alert aggregation to increase user efficiency and reduce effort in the alert analysis.

Segmenting OT networks

Working in conjunction with Forescout eyeSegment, eyeInspect unifies segmentation policies across IT and OT domains. This allows OT asset owners to sync substation segmentation zone structuring in coordination with top-tier cloud and data center environments to better leverage existing investments through seamless and non-disruptive (agentless) integration with current traffic telemetry infrastructure (NGFWs, switches, SDN, cloud, etc.).

Optimize regulatory compliance

The automated asset discovery, continuous monitoring capabilities and flexible reporting features in eyeInspect help electric utilities automate compliance with various regulatory requirements, including NERC CIP in North America and the NIS Directive in Europe. Users can:

- Generate a complete asset inventory list, including all SEL IP-enabled and serial devices
- Monitor host port and services changes

STREAMLINE RISK MANAGEMENT AND NERC CIP COMPLIANCE

Electric utilities are under pressure to streamline risk management and compliance auditing tasks like never before. Forescout helps with the following specific risk management and NERC CIP requirements:

- Asset Baseline Development
- BES Cyber System Categorization
- Security Management Controls
- Personnel & Training
- Electronic Security Perimeters
- Physical Security of BES Cyber Systems
- System Security Management
- Incident Reporting and Response Planning
- Recovery Plans for BES Cyber Systems
- Configuration Change Management and Vulnerability Assessments

- Automate field ports and services scans for BES field devices (relays, RTUs, etc.)
- Provide real-time device and network monitoring with visualizations of all communication paths
- Identify installed patches and applications for all OT Windows devices

Detect and manage risks

By continuously monitoring network communications of thousands of indicators of compromise (IoCs), eyeInspect detects and prioritizes both cyber and operational threats. With our unique user interface and asset map, you can identify the source and path of lateral movement of a threat, while aggregating the threat with other related alerts for detailed remediation and mitigation action. Functioning similar to a pivot table, eyeInspect lets asset owners and analysts quickly drill down or scale up to address incidents holistically with segmentation and policy actions. With the Enterprise Command Center (ECC), eyeInspect supports even more scalability by enabling users to zoom in on alerts from any of their multisite or geo-distributed networks.

eyeInspect uses a wide range of risk management and monitoring capabilities that include:

- Asset baselining per asset or grouped assets
- Active querying for SEL IP-enabled and serial devices
- Advanced alert aggregation for automated remediation
- Patented deep packet inspection (DPI) of 150+ protocols
- Automatic assessment of device vulnerabilities, threat exposure, networking issues and operational problems

MULTIFACTOR THREAT DETECTION

eyeInspect is the first OT network monitoring solution that puts together all these factors and individual data points to assign a single security and operational risk score to each network asset. These risk scores provide a consistent method for finding and prioritizing asset remediation actions. eyeInspect can identify and help remediate a full range of both cyber and operational threats, including:

- Cyberattacks (DDoS, MITM & scanning, etc.)
- Unauthorized network connections, communications
- Suspicious user behavior/policy changes
- Device malfunction or misconfiguration
- New and non-responsive assets
- Malformed protocol messages used in exploits
- Unauthorized firmware downloads
- Usage of insecure protocols
- Default credentials and insecure authentications
- Logic changes
- Visibility to IP-enabled and serial devices

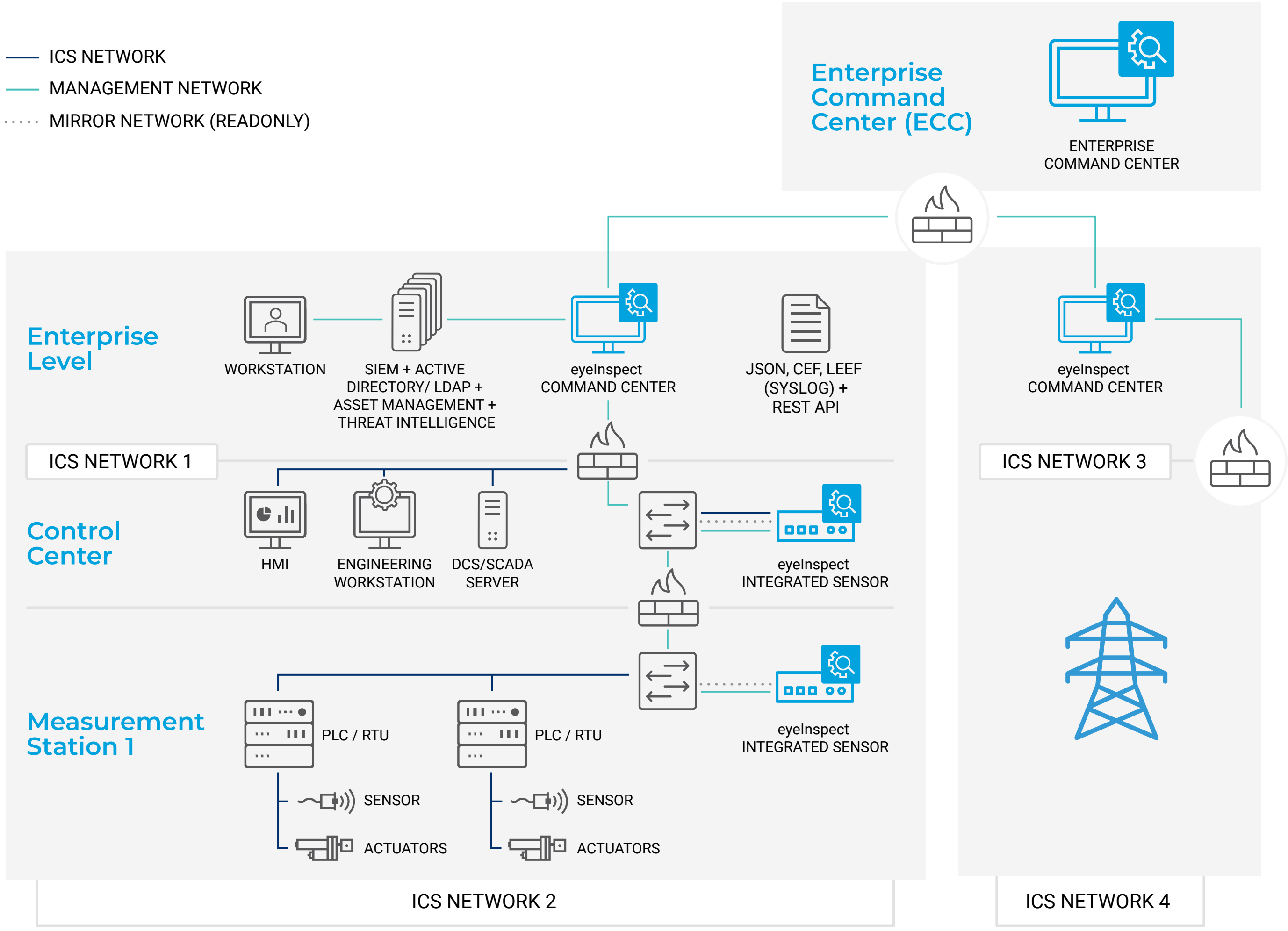
ICS NETWORK
MANAGEMENT NETWORK
MIRROR NETWORK (READONLY)
Enterprise Command Center (ECC)
ENTERPRISE COMMAND CENTER
Enterprise Level
WORKSTATION
SIEM + ACTIVE DIRECTORY/ LDAP + ASSET MANAGEMENT + THREAT INTELLIGENCE
eyeInspect COMMAND CENTER
JSON, CEF, LEEF (SYSLOG) + REST API
eyeInspect COMMAND CENTER
ICS NETWORK 1
ICS NETWORK 3
Control Center
HMI
ENGINEERING WORKSTATION
DCS/SCADA SERVER
eyeInspect INTEGRATED SENSOR
Measurement Station 1
PLC / RTU
PLC / RTU
eyeInspect INTEGRATED SENSOR
SENSOR
SENSOR
ACTUATORS
ACTUATORS
ICS NETWORK 2
ICS NETWORK 4

Figure 1: eyeInspect is part of Forescout's unified IT-OT security platform that provides situational awareness and automated control of both cyber and operational risk across the extended enterprise.

[1] https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa version:1572434569/siemens-cybersecurity.pdf

Don't just see it. Secure it.

Contact us today to actively defend your Enterprise of Things.

forescout.com/platform/eyeInspect

salesdev@forescout.com

toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com